UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,764	02/09/2004	Elias Levy	SYMAP042	8717

21912 7590 06/17/2008
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
BROWN, CHRISTOPHER J	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
06/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/775,764	LEVY, ELIAS	
	Examiner	Art Unit	
	CHRISTOPHER J. BROWN	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-10,13-15 and 17-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-10,13-15 and 17-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 2/26/2008 have been fully considered but they are not persuasive.

Applicant argues that Blake describes using "activity logs" to determine if a "different vulnerability" should be deployed, Blake [0069], but that is not the same as "capturing a state of the honey pot, including by creating a copy of data associated with the honey pot as compromised," as recited in claims 1, 23, and 24.

Examiner argues that the claims must be read with the broadest reasonable interpretation. Blake teaches several activity logs capturing the actions of malicious users, and presenting that information to system administrators to analyze and or take action from. The examiner asserts that this meets the definition of "capturing a state of the honey pot by creating a copy of data associated with the honey pot as compromised"

The applicant also argues that Blake does not teach a "breach" that "indicates the honey pot has become compromised," as recited in claims 1, 23, and 24 as amended. Applicant argues that Blake seems to assume that the "morphing honeypot" has not been "compromised" but instead remains available to lure and monitor attackers.

Examiner argues that even if the applicant does not agree that malicious probing of the honeypot is a "breach", paragraph [0084] describes that the honeypot may be instrumental in a full attack by malicious users. The examiner asserts that a honeypot being probed, or attacked meets the breach and compromised limitations.

Applicant argues the reconfiguring described by Blake occurs over time while the honey pot remains online, which is not the same as "automatically redeploying the honey pot, including by reinitializing the state of the honey pot,"
Examiner argues that the claims must be read with the broadest reasonable interpretation.
The examiners interpretation of the limitation reads on the morphing of the honeypot. When the honeypot changes by morphing, it is reinitialized into a different state. This morphing takes place automatically. Blake teaches in contrast the previous methods of reinitializing a honeypot including taking it offline and restarting it [0036].

The examiner encourages the applicant to include more specific claim limitations consistent with the instant specification to overcome the difference of interpretation.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4, 7, 9, 10, 15, 18-20, 23, 24 rejected under 35 U.S.C. 102(e) as being anticipated by Blake US 2004/0128543.

As per claim 1, 23, Blake teaches deploying a honey pot (Fig 4, system for morphing a honeypot on a dynamic and configurable basis, administrator configures honeypot [0011], [0036]. Blake teaches detecting a breach of the honey pot (suspicious requests, acts to compromise honeypot, client system probing for vulnerability, attacks) [0038], [0070], [0075], [0084]. Blake teaches capturing the state of the honeypot including creating a copy of the data associated with a compromised honeypot (activity logs) [0040]. Blake teaches automatically redeploying the honey pot (automatic reconfiguration operations, reconfigured to present information reflecting a different vulnerability) [0037], [0076].

As per claim 2 Blake teaches analyzing the breach (analysis operations, analyzing requests) [0037], [0075].

As per claim 3 Blake teaches automatically analyzing the breach (automatic analysis), Figure 4, [0037], [0075].

As per claim 4 Blake teaches the breach is automatically detected (determination is made as to whether a probe has been detected) [0070], [0075].

As per claim 7, Blake teaches configuring the honey pot (configuration phase (step 402)) [0037].

As per claim 9 Blake teaches the honey pot is a physical machine (implemented in hardware) [0026].

As per claim 10 The method of claim 1, wherein the honey pot is a virtual machine (virtual directories, emulated)[0038].

As per claim 15 Blake teaches the detecting is based on an elapsed time (track suspicious client requests over time) [0070].

As per claim 18 Blake teaches saving state information associated with the honey pot (activity logs) [0040].

As per claim 19 Blake teaches saving state information associated with the honey pot and wherein saving and redeploying occur in parallel (all activity, actions taken by emulated services, or honeypot as whole, is logged) [0040].

As per claim 20, Blake teaches analyzing the breach and redeploying occur in parallel (analysis and reconfiguration operations performed at the same time) [0037].

As per claim 24, Blake teaches deploying a honey pot (Fig 4, system for morphing a honeypot on a dynamic and configurable basis, administrator

configures honeypot [0011], [0036]. Blake teaches detecting a breach of the honey pot (suspicious requests, acts to compromise honeypot, client system probing for vulnerability) [0038], [0070], [0075]. Blake teaches automatically redeploying the honey pot (automatic reconfiguration operations, reconfigured to present information reflecting a different vulnerability) [0037], [0076]. Blake teaches the honeypot is implemented using a processor and memory coupled to the processor (CPU, disk units) [0026].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blake US 2004/0128543 in view of Fagone US 2004/0078592.

As per claim 6 Blake does not teach shutting down the honey pot.

Fagone teaches shutting down the honeypot (disconnecting from network) [0017].

It would have been obvious to one of ordinary skill in the art to use the shut down method of Fagone in case a honeypot becomes a danger to the network [0017].

Claim 8, is rejected under 35 U.S.C. 103(a) as being unpatentable over Blake US 2004/0128543 in view of Schlereth "Analysis of a Compromised Honeypot on a Cable Modem".

As per claim 8 Blake does not teach copying a honey pot image.

Infocus teaches creating and copying a honeypot image (creating an image of a compromised system for investigation, Pages 21-24).

It would have been obvious to one of ordinary skill in the art to use a honeypot image because it limits the chance of destroying evidence on the compromised system (page 24).

Claims 13, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blake US 2004/0128543 in view of Lewis US 2003/0110396.

As per claim 13 Blake fails to teach detecting is based on the number of outgoing connections detected. Lewis teaches detecting is based on the number of outgoing connections detected (large number of IP requests) [0079].

It would have been obvious to one of ordinary skill in the art to use the detection of Lewis in the system of Blake to detect Denial of Service attack attempts.

As per claim 14 Blake fails to teach detecting is based on the number of incoming connections detected. Lewis teaches detecting a breach based on the incoming connections detected (abnormally large connection attempts to target) [0062].

It would have been obvious to one of ordinary skill in the art to use the detection

of Lewis in the system of Blake to detect Denial of Service attack attempts.

Claim 17, is rejected under 35 U.S.C. 103(a) as being unpatentable over Blake US 2004/0128543 in view of INFOCUS:The Honeynet Project

As per claims 17 Blake does not specify an operating system.

Infocus teaches the honey pot runs a Linux operating system(linux, page 3). It would have been obvious to one in the art to use the multiple OS of Infocus with the honeypot of Blake because it provides support to create a honeypot for a wide range of users.

Claims 21, and 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over Blake US 2004/0128543 in view of Turk US 2005/0108415

As per claims 21, and 22, Blake does not teach mapping an IP address to a honeypot.

Turk teaches receiving an incoming connection associated with an IP address(pinging a given IP address)[0071]. Turk teaches mapping the IP address to the honey pot (honeypot responds to unrouted IP address requests) [0071]. Turk teaches releasing the IP address mapping and mapping another IP address to the honey pot (honeypot accepts any IP address request that is not stored in the routing table, thus it will remap to a different IP if a different unrouted destination IP request arrives) [0071].

It would have been obvious to one of ordinary skill in the art to use the IP mapping of Turk with the system of Blake because it tricks a malicious user into thinking they have successfully compromised their target destination IP.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER J. BROWN whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher J Brown/ 6/15/08
Primary Examiner, Art Unit 2134